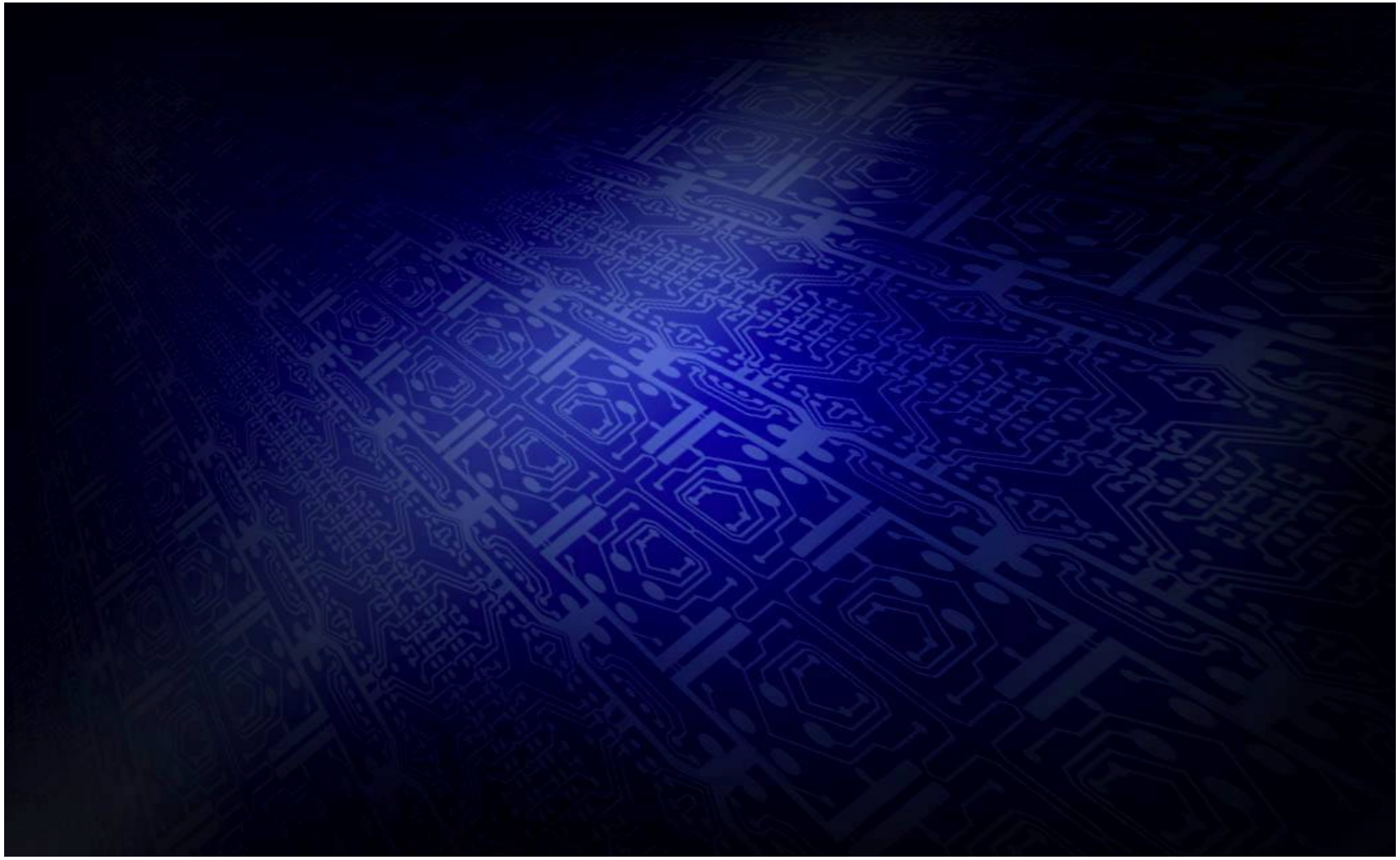
Regional Computer Forensic Laboratory (RCFL)
National Program Office (NPO)

Commonwealth of Virginia

Joint Commission on Technology and Science

September 8, 2004

Search Warrant



What is an RCFL?

- A Regional Computer Forensic Laboratory is:
  - A full service forensic laboratory devoted entirely to the examination of computer evidence in support of criminal investigations
  - A unique law enforcement partnership that promotes quality and strengthens computer forensics laboratory capacity

The RCFL Mission

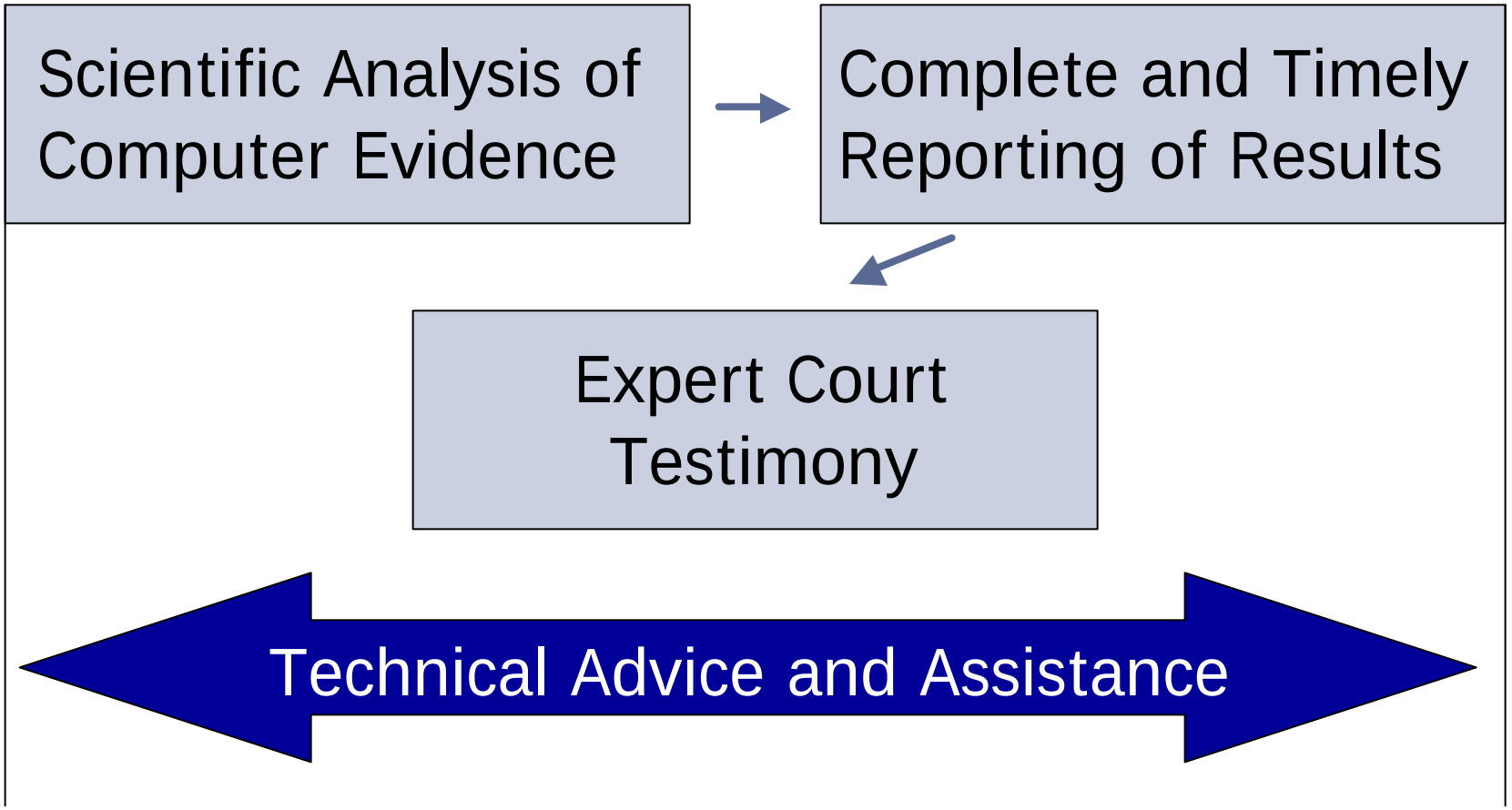
- RCFLs are a critical component in the FBI's effort to support state and local law enforcement
- RCFLs combine the talents and resources of law enforcement agencies at all levels
- RCFLs increase the FBI's ability to investigate criminals and detect and prevent acts of terrorism

RCFL Services

RCFLs Provide these services to their communities

- Conduct forensic exams on all types of digital evidence
- Assist on searches
- Train law enforcement

RCFL Examiner Role



Search and Seizure **Testimony**

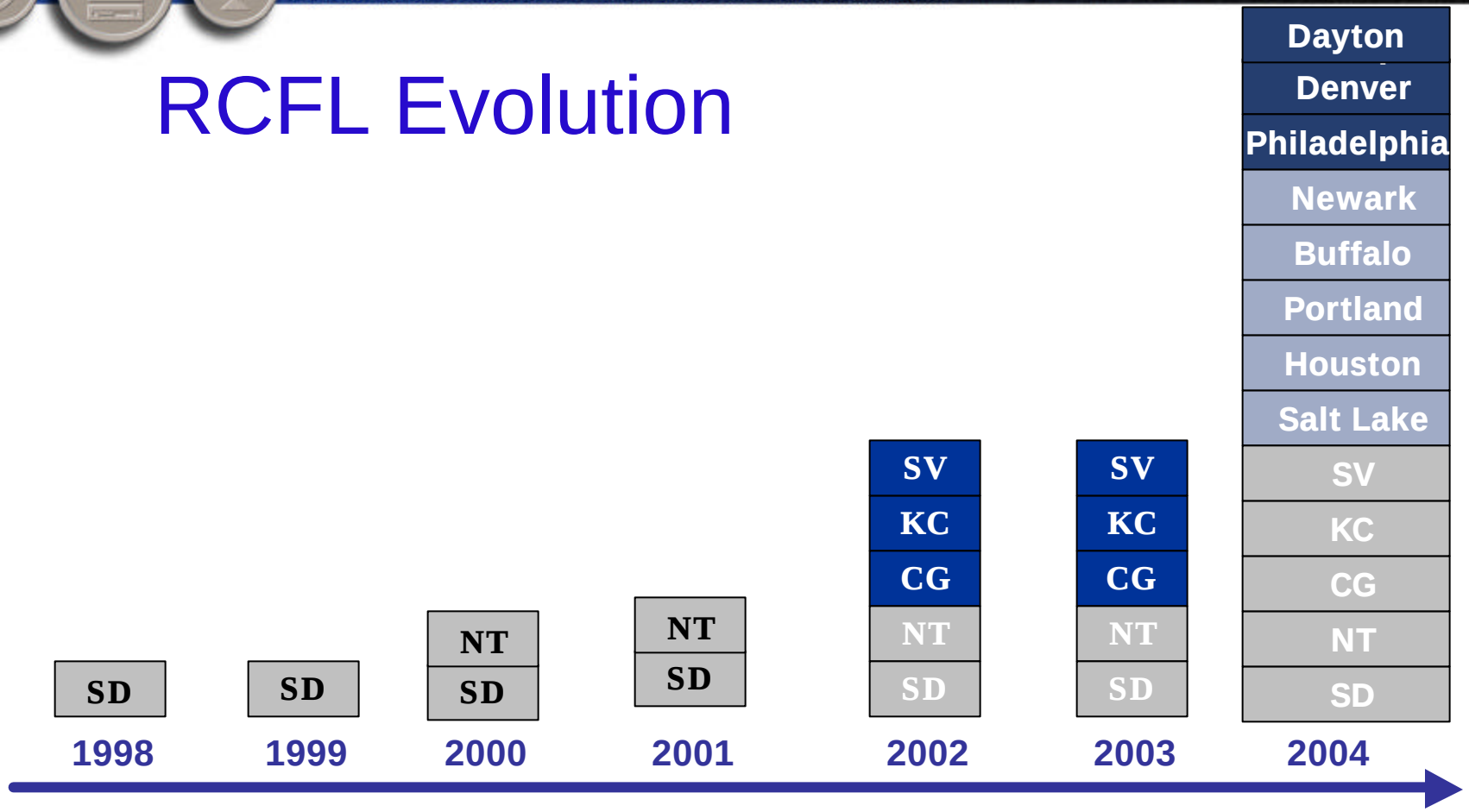
RCFL examiners do not conduct investigations

Examiner Credibility

Examiner credibility relies on *impartial*, *objective* examinations

- ✓ Examiners locate and decipher evidence
- ✓ Examiners *NEVER* interpret evidence

RCFL Evolution



- Initial concept
- AG approval and funding promise
- Funding not provided
- SD fully operational
- Patriot Act
- CT $7.2M supplemental
- Original plan 9-11 labs
- Program Office established
- CG, KC, SF sites selected
- CG, KC open
- New round of selection
- Additional funding

Status of National Program

Location	Status: April 2004
San Diego	Fully operational. Second cohort of state and local examiners being integrated. FY03 service requests: 707
Dallas	Fully operational. FY03 service requests: 461. Moved into new facility in May 2003.
Chicago	Opened in March 03. FY03 service requests: 222
Kansas City	Opened in July 03. FY03 service requests: 76
Silicon Valley, New Jersey, Houston, Salt Lake, Portland	Opening in 2004
Denver, Philadelphia, Dayton, Buffalo	Opening in 2005

Computer/Digital Evidence History

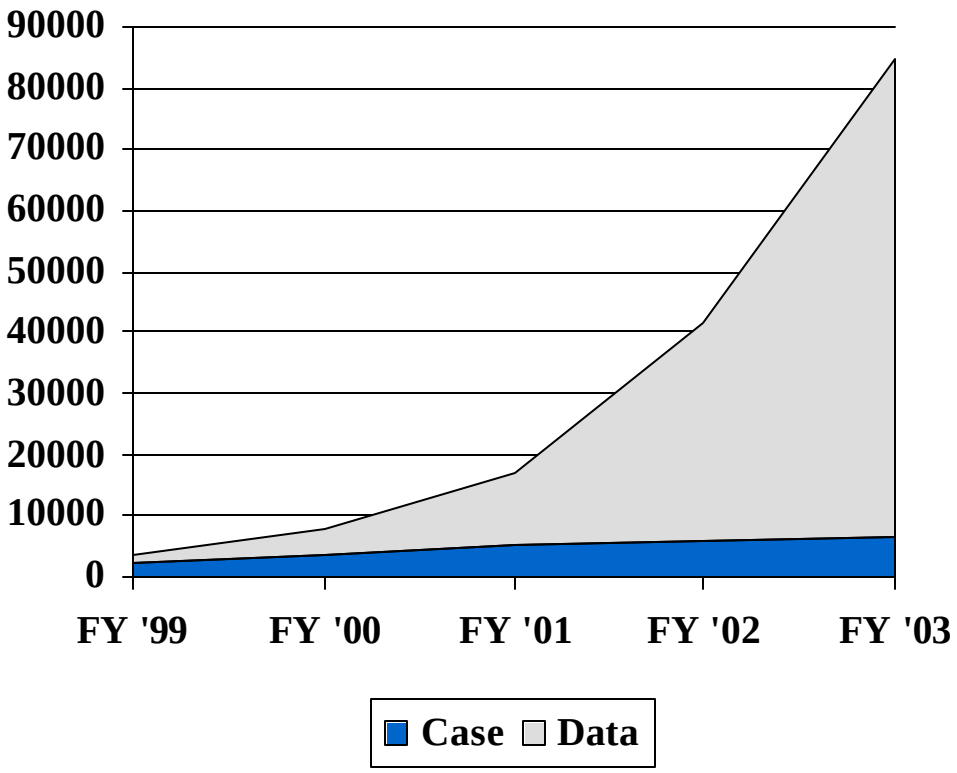
- 1960 2,000 Computers in use in the U.S.A
- 1965 Digital Equipment Co. sells first successful minicomputer for $18,000 each
- 1975 Bill Gates develops idea for Microsoft
- 1976 Steve Jobs exhibits first Apple Computer
- 1984 FBI Magnetic Media Program created, examinations performed in three cases all year
- 1991 Magnetic Media Program becomes CART
- 2000 First FBI RCFL

Response to Increased Demand for Computer Forensic Examination Services

✓Increase the number of trained/certified forensic examiners
✓Increase the number of investigators trained on search and seizure methods
✓Apply technology and tools for process improvement
✓Continue to meet quality standards and gain accreditation
✓Continue to improve efficiency of processes

FBI CART Experience

- Case load:
  - FY ‘99 - 2084 cases
  - FY ‘00 - 3891 cases
  - FY ‘01 – 5166 cases
  - FY ’02 – 5924 cases
  - FY ’03 – 6546 cases
- Data examined:
  - FY ‘99 – 17 terabytes
  - FY ‘00 – 39 terabytes
  - FY ’01 – 119 terabytes
  - FY ’02 – 358 terabytes
  - FY ’03 – 782 terabytes



RCFL Accomplishments at a Glance

FY03 Program Accomplishments

- ✓Processed **82.3** Terabytes of data
- ✓Accepted **1393** requests for service
- ✓Participated in **196** search and seizure operations
- ✓Trained **1525** law enforcement personnel
- ✓Conducted **987** computer forensic examinations
- ✓Served **924** law enforcement agencies in five states

RCFL Governance

National Steering Committee

Represents key stakeholder groups and advises on overarching policy issues

Technical Review Board

Represents the computer forensic technical community and helps set technical operating standards that will meet American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) and/or other standards

Local Executive Boards *(one per RCFL)*

Represent your local participating agencies and provide operational guidance and oversight

National Program Office Role

Start Up	Ongoing Operations
• **Examiner selection** • **Facility coordination** • **Equipment purchase** • **Training coordination** • **Outreach and communications** • **Local executive board facilitation**	• **National Boards** • **Accreditation** • **Ongoing training and certification** • **National conferences** • **Academic outreach** • **Local funding sourcing**

RCFL Resource Requirements

Category	Year 1	Ongoing
Facility buildout	✓	
Facility lease (annual)	✓	✓
Common equipment	✓	
Media and supplies (annual)	✓	✓
Examiner certification training (annual)	✓	✓
Examiner equipment (every two-three years)	✓	✓
Examiner workstation furniture	✓	
TOTAL COSTS	Up to $2 M	~$1 M/yr

Total Lab Funding

State and Local Provisions	RCFL Provisions (through Congressional Funding)	
Personnel	Facility Build-Out	$500,000 (est)
	Facility Lease (annual)	$350,000 - $500,000
	Examiner ▪ Equipment (every 2-3 years) ▪ Training (every year) ▪ Workstations	$42,000/ examiner
	Common Equipment (annual)	$70,000
	Media and Supplies (annual)	$75,000
	Training Room Equipment and Furniture	$150,000

Examiner Training/Certification

A+ Certification Training (2 weeks)

Commercial Vendor

- Training culminates in taking nationally recognized A+ certification test

Basic Data Recovery Analysis (BDRA) (1 week)

National White Collar Crime Center

- Training culminates in end-of-course test

Net+ Certification Training (1 week)

Commercial Vendor

- Training culminates in taking nationally recognized Net+ certification test

FBI Boot Camp (2 weeks)

FBI

- Following the course, examiners conduct competency examination on test hard drive and send results to training coordinator

Moot Court (1week)

- Defense and Prosecuting attorneys query participants on their examination results
- Oral presentation test

Examiners must also conduct five searches and five exams under the supervision of an FBI-certified forensic examiner

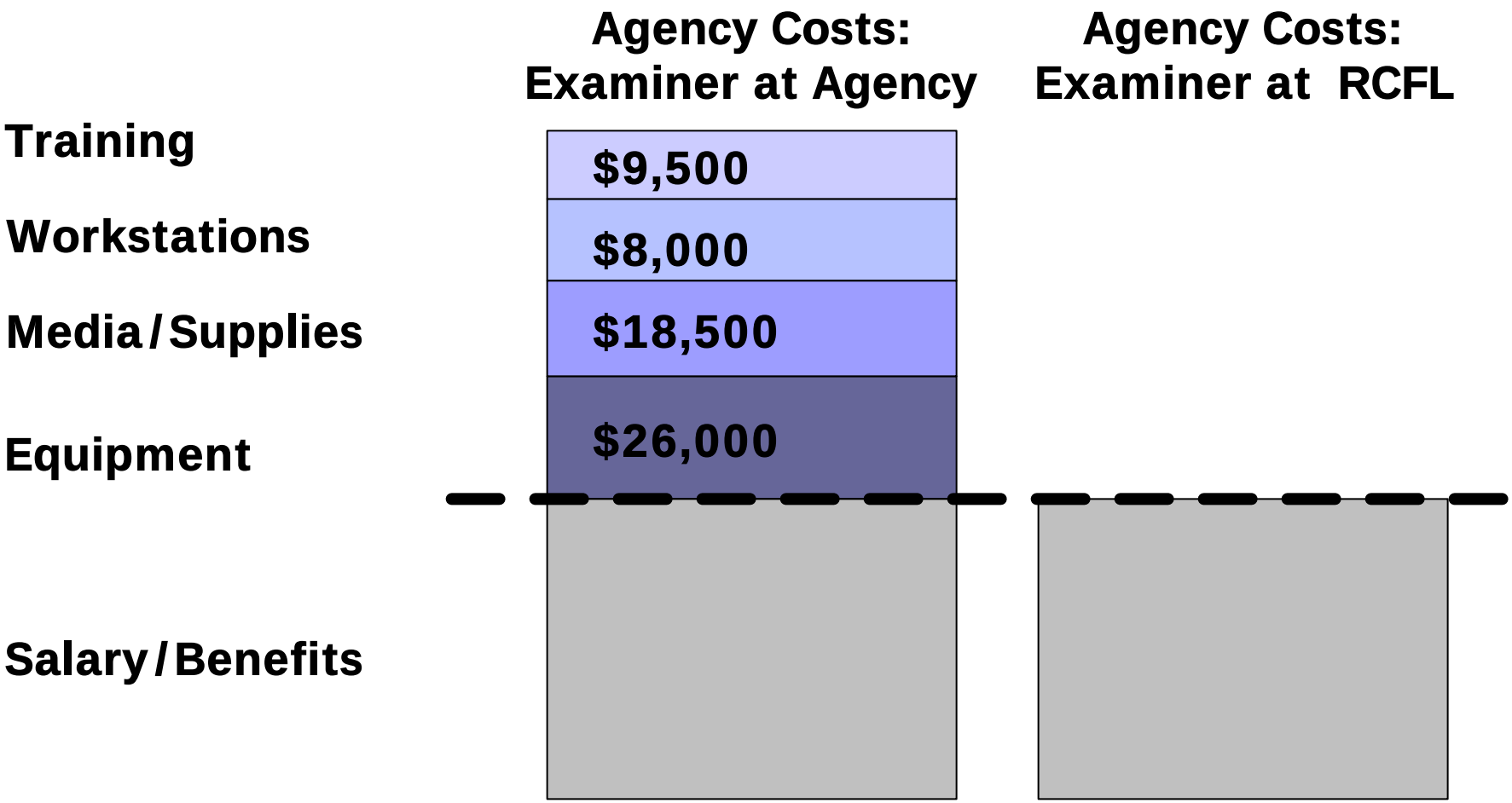
To maintain certification:

- Complete one advanced FBI-sponsored class per year
- Complete two additional outside classes per year
- Pass yearly proficiency test

Benefits of Participation

Agency	Examiner	Community
✓ Computer forensic services and standards ✓ Capability ✓ Training ✓ Knowledge and experience	✓ Training ✓ Networking ✓ Knowledge and experience	✓ Highest quality service ✓ Crisis response capability ✓ Quality law enforcement ✓ National leadership

Cost Benefit to Agencies



Total Agency Cost	**$63,400+Salary**	**Only Salary**

New Initiatives

- Improving efficiency through technology
  - Storage Area Networks
- Expanding examination services
  - PDAs
  - Network forensics
  - Audio/video enhancements

Image Scan

“Crimes Against Children”
Knock and Talks

Boot disk locks suspect’s hard drive

Investigator retrieves active graphics files

Recovering deleted files

- When you delete a file in a Windows 9x system, all you really do is change the first character of the file name in the File Allocation Table (FAT) to the lower case Greek letter sigma.
- The data contained in the file does not change or go away.
- The computer understands that the place where the data for this file resides, may be reused, if needed, but is not overwritten.

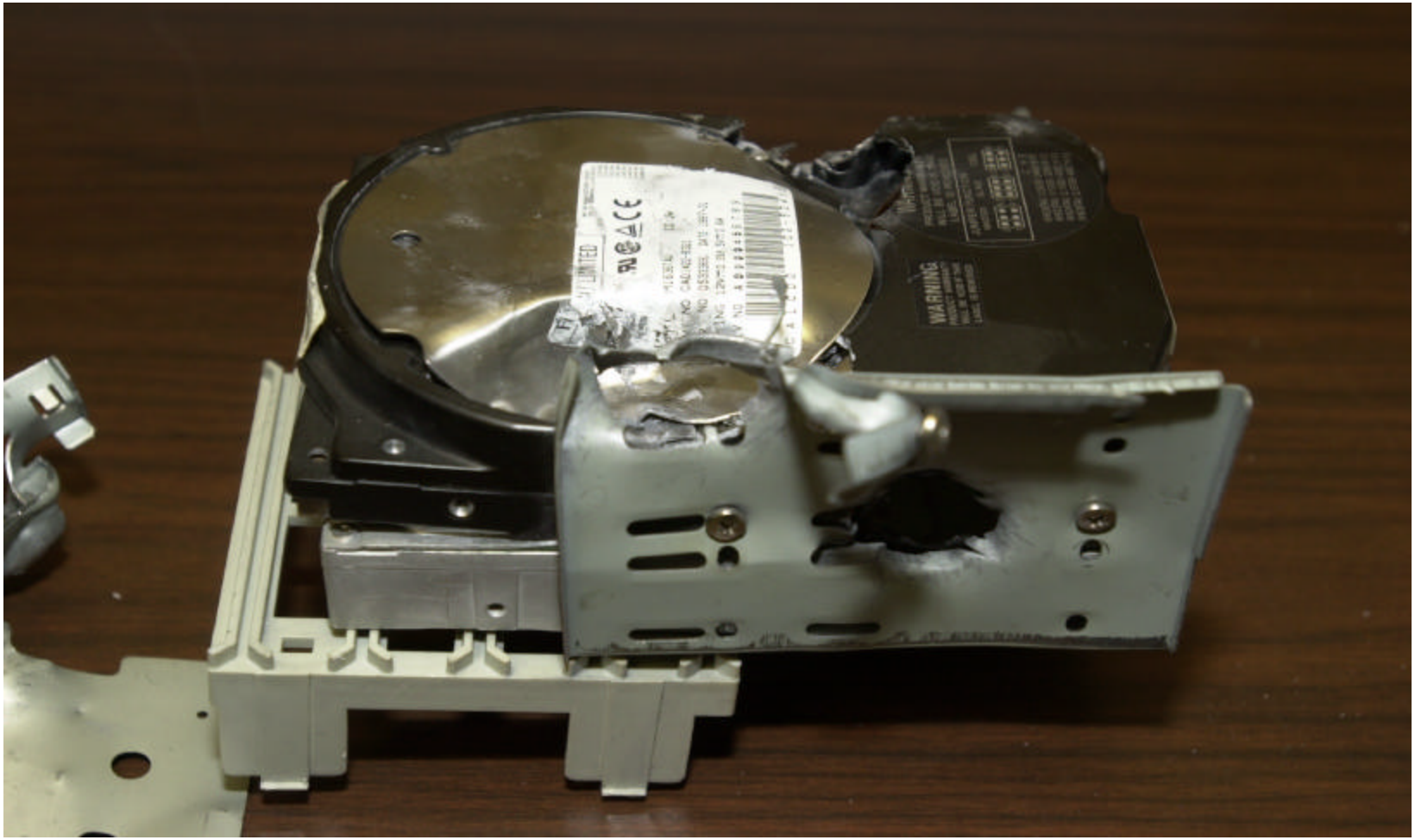
Search Stories 1

- The FBI executed a search warrant at the residence of a suspected child pornographer. When the FBI knocked on the door and announced the search warrant, the subject dropped his laptop computer into the bathtub.
- The laptop was recovered, the water drained, and all data was recovered from the hard drive.

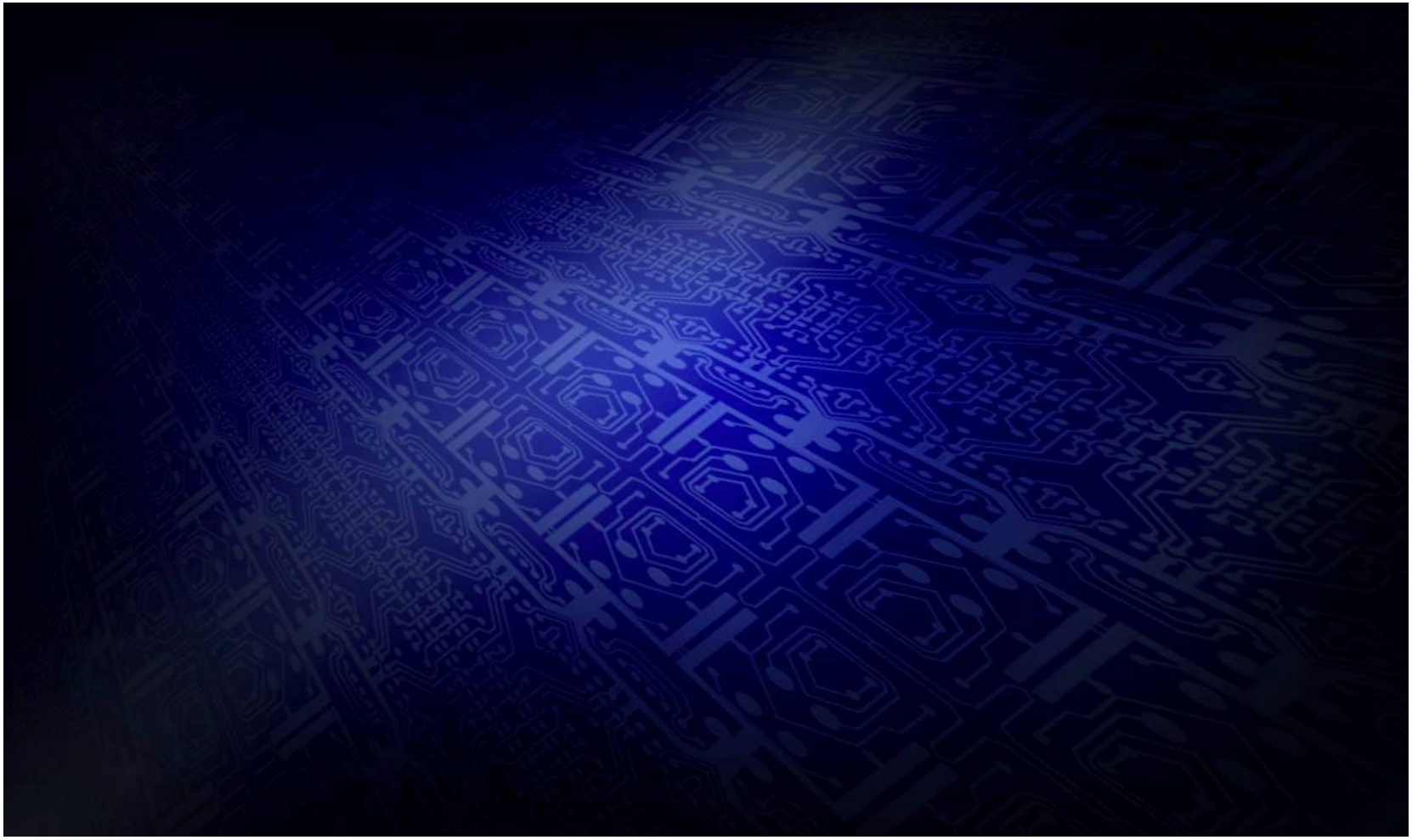
Search Stories 2

- During the FBI's investigation of a child predator, "traveler" case, several floppy disks were recovered from a motel room occupied by a female minor who had traveled from Chicago to Indiana to meet with a man she had met on the Internet. She had used a pen to punch holes through the floppy disk media.
- The FBI took the floppy disks apart, super glued the torn media, ironed the disk, and recovered most of the data from the floppy.

Search Stories 3 (The one that got away)



Your data isn’t safe from hackers!



Questions?

SSA Christ M. Kacoyannakis, Deputy Director

RCFL National Program Office

703-632-2691

ckacoyannakis.cart@fbi.gov

info@nationalrcfl.org

www.rcfl.gov